数据库安全应用服务器的研究与实现*

邵佩英

(中国科学技术大学 研究生院,北京 100039)

E-mail: shaopy@chinainfo.com.cn

摘要: 给出一个经济、实用、有效的安全应用服务器的研制背景、设计方案及其实现技术.该安全应用服务器使得基于美国国防部颁发的可信计算机评估标准和可信数据库管理系统解释中的C2级安全标准的数据库管理系统,达到以强制访问控制为基本特征的B类安全标准.

关键词: 网络环境;数据库安全;强制访问控制;安全应用服务器

中图法分类号: TP311 **文献标识码**: A

1 数据库安全应用服务器(DSAS)的研制背景

1.1 用户对数据库安全的新要求

据调查,目前我国已经建立或正在建立的大、中型信息系统绝大多数都基于网络环境,使用国外研制的数据库管理系统(database management system,简称DBMS).如Oracle,Sybase,Informix,IBM DB2,MS SQLServer等等.它们大都符合美国国防部颁发的可信计算机系统评估标准(trusted computer system evaluation criteria,简称TCSEC)和可信数据库管理系统解释(trusted database interpretation,简称TDI)中的C类安全标准.C类安全标准的基本特征是自主访问控制,自主访问控制允许人们将本来属于自己的访问权限自主地转让给本来无权访问的人,而系统对此却无法进行控制.另外,目前DBMS采用简单的基于用户口令的身份认证,而且口令直接在网络上传输,这是很不安全的,需要改变.

因此,对于高科技、军事、金融等需要高信息安全的领域中的用户来说,C类数据库管理系统已不能满足新的安全要求,需要增强数据库的安全级别,以达到以强制访问控制为基本特征的B类安全标准[1].因为具有B类安全标准的数据库,是通过主体与客体各自所具有的敏感度标记的控制关系来实现强制访问控制的,主体和客体的敏感度标记由系统安全员(system security operator,简称SSO)指派,这种标记不能由用户任意修改,更不能转让,防止了未授权用户的非法入侵.同时,用户也希望能够在保护已有投资的前提下,增强现存系统的安全性,并尽可能地做到改变少、花钱少、见效快.

1.2 增强数据库安全性的方案

增强数据库的安全性使其具有B类安全标准的基本特征有多种方案,最有效的方案是从硬件和操作系统着手,但这将是一项浩大的工程.若从增强数据库管理系统的安全级别着手,又有以下几种方案:

· 引进或购买国外具有B类安全标准的DBMS产品,但由于技术进口上的限制,这些产品尚未进入我国市场;即使可以购买到,经济开销也过大;而且安全性也不一定能够得到保证,因为对一

* 收稿日期: 1999-07-14; 修改日期: 1999-10-10

作者简介: 邵佩英(1941-),女,上海人,教授,主要研究领域为数据库,信息系统,计算机算法语言编译系统.

个国家来说,安全软件总是为保障自己国家的安全而设计的;

• 使用国产 B 类 DBMS,目前正在研制或还需要经受一段时间的考验.而且,现有的大型信息系统大多已经使用国外的 DBMS;

• 在现有的 C2 级安全的 DBMS 基础上,研制一个增强数据库安全的应用服务器,从而达到所期望的 B 类安全标准.

从以上分析可以看出,最后一个方案是实际可行的方案.决定在信息安全国家重点实验室立项,研究采用软件技术,在 C2 级数据库管理系统的基础上,研制一个经济、实用、有效的符合我国国情的增强数据库安全性的软件.这个软件起名为数据库安全应用服务器(database security application server,简称 DSAS),它将使数据库具有 B 类安全标准的基本特征,从而提高信息系统的安全性.从上述背景分析可见,DSAS 的研制不但具有一定的学术意义,而且还具有很好的实际应用价值.

2 网络化环境下数据库安全性需求分析[2]

网络化环境下信息的逻辑安全性环节有:传输信息的安全、存储信息的安全和访问信息的安全.传输信息的安全主要由网络操作系统及其有关传输协议保证,采用以密码学为理论基础的各种数据加密/解密的技术和措施.

数据库及其管理系统作为信息数据的存储地和处理访问地,应能对信息数据的安全存储和安全访问提供服务,并具有安全防范的能力.主要包括:(1) 要求数据库具有保密性,即能防止非法用户的访问,保护数据库中数据的机密不被泄露和篡改;(2) 要求数据库具有完整性和一致性,即能防止对数据库进行不正确的操作或非法用户的恶意攻击;(3) 要求数据库具有可用性,即能防止或及时修复因软、硬件系统的错误所造成的数据库恶性破坏,并拒绝和清除数据库垃圾,使数据库随时保持可用状态;(4) 要求能对数据库变化作跟踪记录,以利于追查并防止否认对数据库的安全责任.

3 DSAS 的设计目标

根据上述分析,确定 DSAS 的设计目标是:在已有的 C2 级 DBMS 的基础上,实现以强制访问控制为主要特征的 B 类安全要求.包括:

(1) 强制访问控制:实现基于敏感度标记的强制访问控制;

(2) 双向身份认证:提供用户与安全应用服务器 DSAS 之间的双向身份认证;

(3) 加密通信:提供安全通信的密钥,保障信道上数据的保密性与完整性;

(4) 增强的安全审计跟踪:增加跟踪记录与安全性有关的操作,以辨清安全责任.

DSAS 作为数据库服务器的特种安全保障软件,用以增强抵御来自系统的外部和内部对数据库安全攻击的内在能力,使计算机信息系统在更安全的数据库环境中运行.

4 DSAS 增强安全性设计原理

DSAS 以 Bell-La Padula 模型作为系统实现的设计基础[3].Bell-La Padula 模型作为实现多级安全策略的形式化安全模型已为各类安全信息系统广为采用.但是,由于 Bell-La Padula 模型设计的出发点是基于孤立系统的操作系统安全,仅关注到可能导致不适当的"泄露"信息的路径,因此,适用于信息的保密[4].根据用户的需求,DSAS 作了相应的扩展.包括:

(1) 信息流动策略

信息流动策略定义为一个格阵$(SC,\angle)$,其中SC为安全类的一个有限集,"$\angle$"表示定义在SC上的二元偏序关系.对于安全类A和B,$A\angle B$表示A类信息的安全级等于或低于B类信息的安全级,允许A类信息流向B类信息.每个安全类定义为$(Level,Scope)$,其中$Level$为密级,$Scope$为领域.设主体S的安全类为$(Level_s,Scope_s)$,客体O的安全类为$(Level_o,Scope_o)$,则有:

• 当且仅当客体O的安全类等于或低于主体S的安全类,即$Level_o\leqslant Level_s$且$Scope_o\subseteq Scope_s$(记为$(Level_o,Scope_o)\angle(Level_s,Scope_s)$)时,主体才能读客体.

• 当且仅当客体O的安全类等于主体S的安全类,即$Level_o=Level_s$且$Scope_o=Scope_s$(记为$(Level_o,Scope_o)-(Level_s,Scope_s)$)时,主体才能写客体.

在本系统中,安全类即安全标记,可分为客体安全标记和主体安全标记两种.

(2) 客体安全标记

为了实现强制访问控制,需要对数据进行安全标记.由于在关系数据库存放信息的组织形式中,元组为基本的信息存取单元,从而实现了元组级的标记,也就实现了最基本的标记方式.在本系统中,选择了基于元组的标记:每一元组附加一个安全标记属性TC,即对关系$R(A_1,A_2,\ldots,A_n)$加元组标记后为$R(A_1,A_2,\ldots,A_n,TC)$,即元组和各个属性的安全级别都是TC.同时,规定增加了安全标记的关系,其新的主键由原主键和TC共同组成.因此,数据库的完整性得到保证.

(3) 主体安全标记

每个主体(用户及其程序)的安全标记称为主体的许可证安全标记,简称许可证.它是由DSAS的系统安全员(SSO)指派给每个用户的,用户自己不能改变,更不能转让.

(4) 安全操作原则

• 当主体试图执行读取操作时,只能读取那些安全标记等于或低于其许可证安全标记的元组(下读).

• 当主体试图执行插入操作时,其许可证安全标记也随之记录到所写元组中,成为该元组的安全标记(该元组的TC的值).

• 当主体试图执行删除操作时,只能删除安全标记等于其许可证安全标记的元组.

• 当主体试图执行替换操作时,只能替换安全标记等于其许可证安全标记的元组.

(5) 身份认证

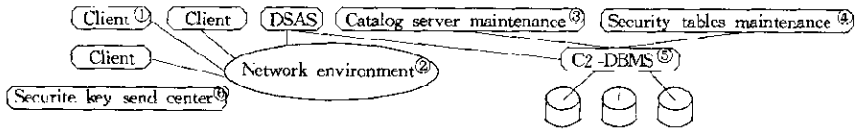
• 随机源使用BBS算法.

• 签名及签名验证算法采用了信息安全国家重点实验室改进后的RSA算法包(1995年通过专家鉴定),进行双向身份认证.

• 采用秘密共享技术来管理系统安全员的密码和服务器私钥(目前采用5选3),从而控制了对单个系统安全员的权限,提高了系统的安全性.

5 DSAS的体系结构

DSAS的总体构成如图1所示,采用客户机/应用服务器/数据库服务器这3层体系结构.其中安全应用服务器DSAS与客户机连接,接受客户机的请求命令,对命令进行安全处理,并负责向客户机返回结果或信息;另一方面,DSAS将从客户机获得的命令经过安全处理后发往数据库服务器,并接收来自数据库服务器的执行结果与各类信息.因此,DSAS既是客户机的服务器,又是数据库服务器的客户机,充当着双重角色.

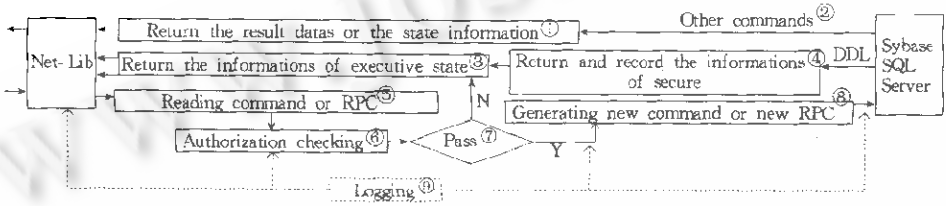


①客户端,②网络环境,③目录服务器维护,④安全表维护,⑤C2级DBMS,⑥密钥分发中心.

Fig. 1 DSAS architecture
图1 DSAS软件的总体结构

6 DSAS 设计目标的实现

(1) 实现基于标记的强制访问控制功能:该功能检查主体对客体的每次访问是否满足基于敏感度标记的强制访问控制条件,如果满足条件,将主体的访问要求传送给数据库服务器执行;否则拒绝传送,并向主体返回信息. 其处理流程如图 2 所示.



①返回结果数据或状态信息,②其他命令,③返回执行状态信息,④安全信息回填,⑤读取命令或RPC,⑥权限检查,⑦通过,⑧形成新命令或RPC,⑨日志记录.

Fig. 2 DSAS processing flow chart
图2 DSAS处理流程

(2) 实现分布式双向身份认证:由于 DSAS 运行在客户机/服务器环境,连接经过网络传输,因此必须包含网络上各用户与服务器之间的双向身份认证. 本系统采用基于 RSA 公钥体制的身份认证方案. 在身份认证过程中要使用用户 ID 号、口令,还需要有用户的公钥和私钥,公钥和私钥对由 SSO 使用独立的专门机制生成并分发给用户. 私钥由用户自己保存,公钥存放在 DSAS 中. 用户个人私钥只限于客户端解密时使用,不发往服务器端,以防止在网络传输中被窃取,从而增强了系统的安全性.

(3) 对 DBMS 数据字典的扩充和修改:为了执行强制访问控制,DSAS 增加了作为数据字典的表,并对现有的数据字典作了必要的修改.

(4) 安全检查与 SQL 语句处理:安全应用服务器 DSAS 对用户发送的 SQL 命令进行专门的强制访问控制检查. 检查通过,将命令传给数据库服务器,由数据库服务器负责对其进行自主访问控制的检查,并执行命令,同时把结果数据或信息发送给 DSAS 进行处理(如图 2 所示).

由于用户是通过 SQL 语句或存储过程来访问数据库服务器的,为了使 SQL 语句对 DSAS 的强制访问安全标记属性给予完备支持,有必要对各类 SQL 语句作安全性分析,并根据分析结果对 SQL 语句或存储过程分别作出相应的处理.

7 结束语

DSAS 安全应用服务器作为增强数据库管理系统安全性的软件系统,利用三层体系结构,可以保证对客户机和后台服务器的较少改动,并以对用户透明的方式增加安全功能,具有很好的实用价值.

现在,DSAS 已经通过信息安全国家重点实验室组织的专家鉴定. 专家们认为:DSAS 设计思

想新颖、合理,既保护了现有投资又增强了数据库安全性,实现了设计目标,达到了 TCSEC 和 TDI 的 B 类安全标准的基本特征,具有一定的创新性和实用性,居国内领先.目前的工作是,正在进一步完善 DSAS,使其能形成产品,推向社会.

References:

[1] Trusted computer system evalution criteria. DOD 5200. 28-STD, USA, 1985.

[2] Adams, D. A., Pappa, S. R. Issues in Client/Server Security. Information System Security, 1995. 27~41.

[3] Bell, D. E., Lapadula, L. J. Secure computer system: unified exposition and multics interpretation. The MITRE Corp., 1976.

[4] Hong, Fan, Cai, Wei, Yu, Xiang-xuan. One improve on the Bell-La Padula model for multilevel security database system. Chinese Journal of Computers, 1995,18(10):763~768 (in Chinese).

附中文参考文献:

[4] 洪帆,蔡蔚,余祥宣.一个用于安全数据库系统的改进 Bell-La Padula 模型.计算机学报,1995,18(10):763~768.

Research and Implementation of Database Security Application Server

SHAO Pei-ying

(*Graduate School of Beijing University of Science and Technology of China, Beijing* 100039, *China*)

E mail: shaopy@chinainfo.com.cn

Received July 14, 1999; accepted October 10, 1999

Abstract: The development background, the design and the implement technology of a database security application server are presented in this paper, which can realize important security characteristics of B kind of TCSEC (trusted computer system evaluation criteria) and TDI (trusted database interpretation). It is an economical, practical and effectual method.

Key words: network environment; database security; mandatory access control; security application server